IN THE CLAIMS

1. (Currently Amended) A system for distributing authentication information to a remote device, comprising:

~~a computer-readable~~ an authentication information store on a computer-readable memory configured to store authentication information for a plurality of users; and

a data processor executable authentication system configured to receive from the remote device a request for authentication information for one of the plurality of users;

wherein the request comprises identity information for use in determining whether the request is from one of the plurality of users,

wherein the authentication system retrieves from the authentication information store, based on the identity information, the authentication information for the one of the plurality of users ~~from the authentication information store~~;

wherein the authentication information for the one of the plurality of users is present in the authentication information store prior to receipt of the request for authentication information;

wherein the retrieved authentication information is provided to the remote device for use in authenticating a user that is requesting remote access to a computer network.

2. (Previously Presented) The system of claim 1, wherein the authentication information is used in a two-factor authentication scheme.

3. (Currently Amended) The system of claim 1, wherein the authentication information store comprises a seed store configured to store a plurality of seeds; and

wherein the authentication system is configured to: receive from the remote device a seed request for a one of the plurality of seeds~~from the remote device~~, the seed request including ~~which includes an~~ a received access code;[[,]] ~~in order~~ to retrieve the one of the plurality of seeds from the seed store;[[,]] to calculate [[~~an~~]]a calculated access code using the retrieved seed;[[,]] to determine whether the calculated access code matches the received access code;[[,]] and to return the retrieved seed to the remote device ~~where~~ if the calculated access code matches the received access code.

4. (Original) The system of claim 1, wherein the request comprises a Hypertext Transfer Protocol (HTTP) connection request.

5. (Currently Amended) The system of claim 1, wherein the request comprises a network password and a digital signature, and wherein the network password and digital signature are verified by the authentication system before the authentication information is provided to the remote device.

6. (Previously Presented) The system of claim 1, wherein the identity information comprises user information and account information.

7. (Previously Presented) The system of claim 6, wherein the identity information identifies a particular user and corresponding authentication information being requested, and is used by the authentication system to authenticate the user requesting the authentication information.

8. (Previously Presented) The system of claim 1, wherein the identity information in the request is used by the remote device for two-factor authentication.

9. (Previously Presented) The system of claim 8, wherein the identity information comprises a network password entered by the user of the remote device and a digital signature generated based on a transformation of at least a portion of the information in the request, a signature key, and a signature algorithm.

10. (Currently Amended) The system of claim 1, wherein the authentication system does not provide the authentication information to the remote device ~~because~~ if a match was not found in the authentication information store based upon the identity information.

11. (Withdrawn) The system of claim 1, wherein the authentication information comprises a password required for remote access to resources in the computer network, wherein the password is not known to a user of the remote device but is required for access to the resources in the computer network.

12. (Withdrawn) The system of claim 1, wherein the authentication information comprises an access code required for remote access to resources in the computer network, wherein the access code is not known to a user of the remote device but is required for access to the resources in the computer network.

13. (Withdrawn) The system of claim 1, wherein the retrieved authentication information comprises an expiring password which is valid for a period of time.

14. (Withdrawn) The system of claim 13, wherein the period of time is on the order of minutes.

15. (Withdrawn) The system of claim 1, wherein the retrieved authentication information comprises an expiring access code which is valid for a period of time.

16. (Withdrawn) The system of claim 1, wherein the retrieved authentication information comprises a non-expiring password and is stored in a protected data store on the remote device.

17. (Currently Amended) The system of claim 1, wherein the retrieved authentication information comprises a seed from which access codes are to be generated by the remote device, and wherein the seed is stored in a protected data store on the remote device.

18. (Previously Presented) The system of claim 1, wherein the remote device uses the retrieved authentication information to gain access to a corporate local area network (LAN).

19. (Currently Amended) The system of claim 18, wherein two-factor authentication is used in the LAN to authenticate a user requesting remote access to the LAN, and wherein the retrieved authentication information is used in performing two-factor authentication in order to gain access to the LAN.

20. (Currently Amended) The system of claim 19, wherein the retrieved authentication information comprises a seed which a two-factor code generator of the remote device ~~device's two-factor code generator~~ uses to produce an access code, wherein the access code is also based upon a value provided by the remote device's clock, wherein the access code is used by the remote device to gain access to the LAN;

wherein the seed is used by the authentication system to also generate an access code for use in a comparison with the access code generated by the remote device; and

wherein access to the LAN is either granted or denied based upon the comparison.

21. (Original) The system of claim 20, wherein the remote device only generates the access code when access to the LAN is requested by the user of the remote device.

22. (Previously Presented) The system of claim 20, wherein the authentication information store comprises an index by user name that indicates users authorized for remote access to the LAN.

23. (Previously Presented) The system of claim 22, wherein the authentication information store stores user seed values from which access codes are to be generated .

24. (Original) The system of claim 1, wherein the remote device is a wireless mobile communication device.

25. (Original) The system of claim 24, wherein the remote device stores the authentication information in a data store.

26. (Original) The system of claim 25, wherein the data store is implemented in a smart card.

27. (Original) The system of claim 25, wherein the data store is implemented in a Universal Serial Bus (USB) token.

28. (Original) The system of claim 1, wherein the remote device is a desktop computer.

29. (Currently Amended) The system of claim 1, wherein the remote device communicates with the authentication system over a communication system, and wherein the communication system comprises a wide area network (WAN) and a wireless network gateway.

30. (Currently Amended) A method of distributing authentication information for remotely accessing computer resources, comprising:

receiving a request for the authentication information from a remote device, the request comprising identity information of a user of the remote device;

wherein the authentication information is stored in an authentication data store;

authenticating the user based on the identity information in the request; and

returning the authentication information to the remote device to authenticate a user requesting remote access to a computer resources based upon the returned authentication information;

wherein the authentication information is present in the authentication data store prior to receiving the request for the authentication information.

31. (Currently Amended) An apparatus for use in handling authentication information for a user of a remote device, comprising:

~~a computer-readable~~ an authentication information store on a computer-readable memory configured to store authentication information for the user of the remote device, the authentication information provided by a remote authentication system;

wherein a request for the authentication information from the remote device to the remote authentication system contains identity information;

wherein the authentication information that is stored in a data store by the remote authentication system is provided to the remote device after the request is processed based upon the identity information contained in the request;

wherein the authentication information is present in the authentication information store prior to receipt of the request;

a data processor executable code generation system configured to retrieve the authentication information stored in the authentication information store;

wherein access information is generated based upon the retrieved authentication information and is used to authenticate a user requesting remote access to a remote computer network.

32. (Currently Amended) A method for obtaining authentication information for use in remotely accessing a computer network, the method comprising:

providing a request from a user of a remote device to an authentication system for the authentication information that is stored in a data store by the authentication system;

wherein the request comprises identity information for use by the authentication system to authenticate the user based on the identity information provided in the request;

receiving by the remote device the authentication information from the authentication system;

wherein the received authentication information is used to authenticate a user requesting remote access to the computer network;

wherein the authentication information is present on the data store prior to the providing a request from a user.

33. (New) The system of claim 1, wherein the authentication information store is on a non-volatile memory.